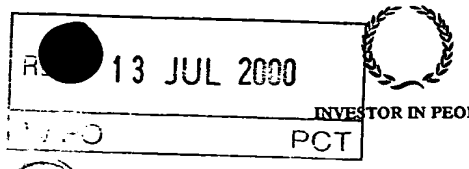


The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

09/936413

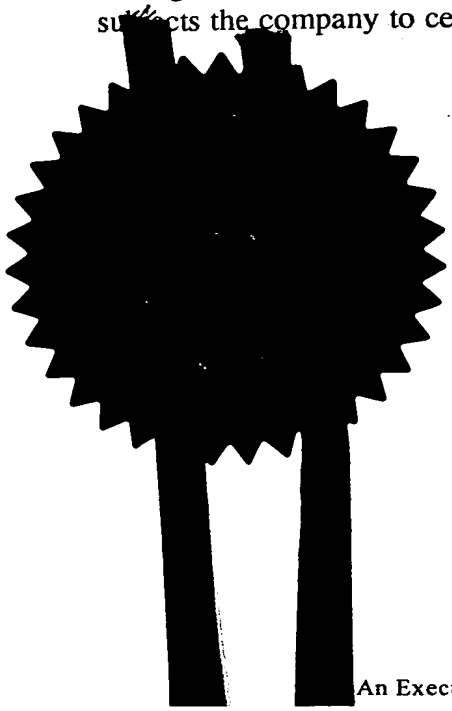
PCT GB00/00767

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

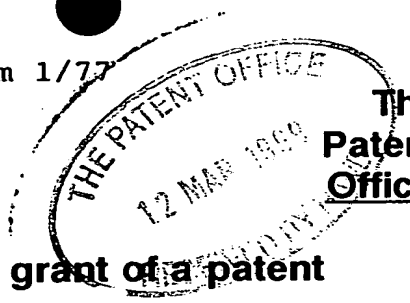


Signed J Evans.

Dated - 4 JUL 2000

CERTIFIED COPY OF PRIORITY DOCUMENT

Patents Form 1/77
Patents Act 1977
(Rule 16)



The Patent Office

15MAR99 E432473-3 D02917
P01/7700 0.00 - 9905777.0

Request for grant of a patent

The Patent Office
Cardiff Road
Newport
Gwent NP9 1RH

1. Your reference
5296201/JDC

2. Patent Application Number
9905777.0

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

University College London
Gower Street
London WC1E 6BT

Patents ADP number *(if known)* 7976520002

If the applicant is a corporate body, give the country/state of its incorporation
Country:
State:

4. Title of the invention

A METHOD AND APPARATUS FOR GENERATING MULTIPLE WATERMARKED COPIES OF AN INFORMATION SIGNAL

5. Name of agent
Beresford & Co

"Address for Service" in the United Kingdom to which all correspondence should be sent
2/5 Warwick Court
High Holborn
London WC1R 5DJ

Patents ADP number 1726001

6. Priority details

Country	Priority application number	Date of filing

Patents Form 1/77

7. If this application is divided or otherwise derived from an earlier UK application give details

Number of earlier of application | Date of filing

8. Is a statement of inventorship and or right to grant of a patent required in support of this request?

YES

9. Enter the number of sheets for any of the following items you are filing with this form.

Continuation sheets of this form	
Description	34
Claim(s)	18
Abstract	1
Drawing(s)	11 + 11

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	ONE
Request for Substantive Examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application

Signature Beresford & Co BERESFORD & Co Date 12 March 1999

12. Name and daytime telephone number of person to contact in the United Kingdom

Dr John Collins

Tel:0171-831-2290

A METHOD AND APPARATUS FOR GENERATING MULTIPLE WATERMARKED COPIES OF AN INFORMATION SIGNAL

The present invention generally relates to a method of watermarking an information signal to generate multiple different watermarked copies of the information signal.

When a provider of electronic information such as audio, video, TV, images, and documents wants to be able to identify when illegal copies of the electronic information have been made, it is well known in the art that the electronic information can be watermarked to include information identifying the recipient of the information e.g. a unique user ID that does not perceptually alter the quality of the electronic information. Further, in order to reduce the likelihood of being able to circumvent the watermarking security labelling of the electronic information, the watermarking technique should not be evident in the electronic information. There are many different ways known in the art for carrying out watermarking of electronic information and the techniques employed will in part depend upon the type of electronic information. For example, one form of watermarking documents is to vary spaces within the documents in accordance with a particular algorithm. For audio data, the audio signal

can be modified in an inperceptible manner in order to provide the watermarking. For images which have been compressed using the JPEG compression technique, the images can be watermarked by varying the compression parameters. This can similarly be applied to MPEG compression parameters for video images.

In conventional watermarking techniques, multiple copies of the electronic information are required for multiple recipients, in order to ensure that it is possible to trace the origin of each copy made in the event that illegal copies are detected in circulation. Each copy must be uniquely watermarked to identify the source of any illegal copies.

Electronic information is commonly transmitted from an information source to a recipient over a network. Examples of such networks are a cable network and the Internet or an intranet. Where a copy is transmitted specifically to a recipient from the source (i.e. a unicast transmission) the source can watermark the electronic information transmitted to the recipient with information identifying the recipient so that in an event illegal copies are detected, the source of the copies can be determined from the watermark.

In networks it has become very common for information to be sent to more than one recipient at a time and this is termed multicast transmission. Multicast transmission over networks has the advantage

over unicast transmission in that the sender need only transmit a single copy which is transmitted to multiple recipients. However, because the source only transmits a single copy, it has not been possible using the multicast transmission of the prior art for each recipient to receive a uniquely watermarked copy of the electronic information.

In multicast sessions over networks, conventionally a recipient will subscribe to the transmission and thus the source is able to transmit the electronic information in an encrypted form. The subscribers are given the key to decrypt the electronic information when they receive it. This offers security in that only recipients which have the key are able to decrypt the electronic information. This does not however prevent illegal copies being made of the legitimately received and decoded electronic information. It would however, be of great benefit to be able to trace the origin of any illegal copies. In the Internet, because routers in the Internet are required to route electronic information, possible sources of illegal copies of the electronic information include not only the legitimate recipients, but also network operators having control over the routers through which the electronic information passes.

The present invention provides a method of watermarking an information signal to generate multiple different watermarked copies of the information signal.

The information signal is segmented into information segments and a plurality of differently watermarked versions of each information segment are generated. One of the watermarked versions of each segment for each one of the multiple different copies to be generated is selected to generate a sequence of differently watermarked segments for each copy. The sequence is probabilistically unique for each copy. The selection is controlled on the basis of information on the identity and/or location of the receivers of each copy.

Thus in accordance with the present invention each copy of the information signal is watermarked using a unique sequence of watermarks. This has the benefit that the number of watermarked versions of each information segment need not be as large as the number of copies to be made. This reduces the amount of processing required in order to generate the watermarked information signals for the receivers.

Although the present invention is applicable to unicast transmission, the present invention is particularly beneficial when used with multicast transmissions over a network. In such an embodiment of the present invention, the intelligence available at nodes in the network is utilised to carry out the selection process. The source of the information signal generates the plurality of differently watermarked versions of each segment of the information signal. These

are transmitted to a node in the network. Each node in the network then selectively filters out one of the watermarked versions of each segment dependent upon the position of the node in the tree and the path down which the information signal is to be transmitted before passing the packet downstream. This selection is preferably carried out pseudo-randomly using the information on the network node position and path as a key for the pseudo-random number generation.

In an embodiment, at the final node in the network before a receiver, the selection takes the form of the selection of only one of the watermarked versions of each segment to be transmitted to the receiver so that the receiver only receives one watermarked version of each segment. The selection process in this final node is additionally dependent upon information identifying the receiver.

Thus in a network embodiment, because at network receiver nodes more than one user or subscriber may be operating (i.e. there can be more than one receiver at a physical location in the network), information uniquely identifying the receiver (user or subscriber) is required to be able to more accurately trace the source of illegal copies of the information signal in addition to location information (i.e. the route information). The use of both routing information and user identity information enables the recipient to be identified where illegal

copies have originated from recipients and where illegal copies have originated from within the network the routers responsible can be identified from the routing information.

The number of differently watermarked versions of each segment generated by the watermarking means is dependent upon the number of nodes in the network. Because each node in the network filters out at least one of the watermarked versions, in order for there to be at least two watermarked versions received by the final node in the network to which a receiver is connected, the number of generated watermarked versions must be greater than the longest route between the source and a receiver i.e. a route having the largest number of nodes. Because in IP (Internet Protocol) multicast sessions in particular, receivers are able to actively join and leave multicast sessions, the longest route in a multicast session may vary during the session. Thus, information on the number of nodes in each route between the receivers and the source is monitored at the source so that the number of differently watermarked versions of each segment of the information signal can be varied as necessary. If, during the transmission of an information signal, the number of differently watermarked versions of the segments is changed, the point during the information signal at which the change occurs must be noted at the source because this will affect the sequence

of watermarked versions appearing in the copy of the information signal received by each receiver and will thus be required to trace the origin of illegal copies.

In accordance with an aspect of the present invention, the origin of copies of the information signal can be detected by using stored information on the identity of the recipients, and a copy of the information signal. By applying the watermarking and selection procedure to the original information signal and comparing it with the copy to be checked, it is possible to identify the receiver from which the copy originated.

In the embodiment wherein the selection process is carried out by the nodes in the network, the information required in order to identify the origin of a copy is information on the identity of the receiver and information on the route taken by the copy through the network. This information is stored during transmission to be used if necessary to trace the origin of suspected illegal copies.

Embodiments of the present invention will now be described with reference to the accompanying drawings, in which:

Figure 1 is a functional diagram of the present invention;

Figure 2 is a schematic diagram of an example of a network in which a source S multicasts an information signal to a plurality of receivers R_1 to R_7;

Figure 3 is a schematic diagram of the network tree structure of the network of Figure 2;

Figure 4 is a flow diagram of the steps carried out at a router in the configuration of the network to carry out the selection process in accordance with an embodiment of the present invention;

Figure 5a is a flow diagram illustrating the steps carried out at routers in the network to pass packets onto other routers in accordance with an embodiment of the present invention;

Figure 5b is a flow diagram illustrating the steps carried out by a final router to pass packets onto a receiver in accordance with an embodiment of the present invention;

Figure 6 is an illustration of the structure of the watermarked data generated by the source in accordance with an embodiment of the present invention;

Figure 7 is an illustration of an example of the data structure received by a receiver in accordance with an embodiment of the present invention;

Figure 8 is a diagram of the tree structure of the network of Figure 3 illustrating the flow of packets over the network to the receivers in accordance with an embodiment of the present invention;

Figure 9 is a flow diagram illustrating the steps carried out when a new subscriber wishes to join a multicast session in accordance with an embodiment of the present invention;

Figure 10 is a schematic diagram of the structure of the source apparatus for the information signal in accordance with an embodiment of the present invention;

Figure 11 is a schematic diagram of a router in accordance with an embodiment of the present invention; and

Figure 12 is a flow diagram of the analysis method of an embodiment of the present invention.

GENERAL OVERVIEW OF THE PRESENT INVENTION

Figure 1 illustrates the functional components of a generalised embodiment of the present invention. An information signal source 2 provides the information signal for which multiple unique watermarked copies are required. An information segmenter 3 segments the information signal from the information signal source 2 and inputs this into a watermarking module 4 which will carry out the watermarking of the information segments. The watermarking module 4 generates a plurality of differently watermarked copies of each segment using watermarking parameters stored in the watermarking data store 1. The plurality of differently watermarked copies of each information segment are then received by a

selector 5 which selects a watermarked copy for each of the information segments for each of a plurality of receivers 7 in dependence upon information on the receivers 7 stored in the receiver data store 6. Thus, the selector 5 will generate M unique sequences of differently watermarked segments from a stream of information segments each having N different watermarked copies. The benefit of the present invention is that the number N of differently watermarked sequences generated in the watermarking module 4 is less than the number M of uniquely watermarked copies of the information signal generated and received at the receivers 7 i.e. $M \gg N$.

The processing required in the generation of the multiple uniquely watermarked copies is thus greatly reduced because the watermarking operation is carried out less times. The selection of watermarked copies of each segment is a simple operation which is not computational intensive compared to the generation of watermarked copies. The present invention thus provides for a considerable reduction in processing requirements particularly when $M >> N$.

An analyser module 8 is also provided to enable illegal copies of the information signal to be analysed to identify the receiver from which it originated. The analyser module needs to have copies of the information signals received by the receivers 7. These can either

be provided directly by the selector 5 or using information from the receiver data store 6, the watermarking data store 1, and the information signal source 2, they can be reconstituted to predict what information signals would have been received by the receivers 7. An input device 9 is provided to allow the input of the alleged illegal copy of the information signal into the analyser module 8 for comparison with the predicted copies of the information signal for receivers. The comparison will determine from which receiver the alleged illegal copy originates.

EMBODIMENT OF THE PRESENT INVENTION

An embodiment of the present invention will now be described with reference to Figures 2 to 12.

This embodiment of the present invention is applied to the multicast transmission of an information signal over an IP (Internet Protocol) network such as the Internet or an intranet.

As will be described hereinafter, this embodiment of the present invention particularly benefits from the advantages of the present invention because the processing required to select the watermarked copies of each segment is distributed among the nodes of the network. Thus, a further computational saving is provided in that the source need only generate the N multiple watermarked version of each segment without actually

generating the unique watermarked copy for each receiver. This embodiment to the present invention is able to achieve this because of the intelligence which can be made available within routers in IP networks.

Figure 2 is a schematic diagram of an IP network in which a source S multicasts an information signal over the network to receivers R_1 to R_7 who subscribe to the multicast session. The source S is arranged on a local area network 10 which has an interface to a node N_1 (a router) in the network. The node N_1 has IP connections to two other nodes N_2 and N_3. The node N_2 has IP connections to two receivers R_1 and R_2, as well as a connection to another node N_A and to node N_4. Node N_A has a connection to other nodes (not shown) and to a node N_B which interfaces to a local area network (LAN) 11. In the LAN 11 there are no receivers which have subscribed to the multicast session.

The node N_3 has an IP connection to a node N_5 which in turn has an IP connection to a receiver R_5, an IP connection to other nodes (not shown) and an IP connection to node N_6. Node N_6 has IP connections to two receivers R_6 and R_7 and IP connections to other nodes (not shown). Node N_4 has IP connections to four receivers only two of which R_3 and R_4 are subscribers to the multicast session.

In a multicast session of this embodiment, when the source wishes to initiate a multicast session, a source path message (SPM) is transmitted to the node N_1 which broadcasts the SPM to the other nodes in the network. This enables the nodes to identify the path of the multicast session. For example, in node N_4 there are two possible paths from nodes N_2 and N_3. However, the IP connection to N_3 is preferred for example because it is shorter and thus the IP connection between N_2 and N_4 is dropped for the multicast session. On nodes N_A and N_B there are no subscribers requiring receipt of the multicast information and thus nodes N_A and N_B play no part in the multicast session: they do not require the information signal to be transmitted to them. If a new subscriber on the LAN 11 were to request to join the multicast session, the node N_B will know the route back to request connection to the multicast session and will thus connect to node N_A which in turn will connect to node N_2 thus forming a route to the new receiver on the LAN 11. Thus the nodes in the network store information on multicast sessions and IP connections to enable a receiver to subscribe and join a multicast session which can entail the opening up of new routes through the network.

The routes taken by information signals through the network can thus be redrawn as a tree structure as

illustrated in Figure 3. Nodes which are not in the communication route between the source and the receivers are not relevant as will become clearer hereinafter. At each level in the tree a node is assigned a unique label. Each level corresponds to a number of "hops" between nodes. In Figure 3 the letters indicate the interface IP addresses. Thus node 1 is labelled *ab*, node 2 is labelled *abce*, node 3 is labelled *abdf*, node 4 is labelled *abdfkm*, node 5 is labelled *abdfer* and node 6 is labelled *abdflrtv*. These labels are determined by the nodes from their position in the network using the source path message. The method by which the labels are determined will now be described with reference to the flow diagram of Figure 4.

Figure 4 is a flow diagram illustrating the steps carried out at each router in order to set up the router ready to receiver and filter the information signal. A source path message (SPM) is transmitted by the source which wishes to set up a multicast session. This is then received by the first hop router and it propagates through the network from router to router as will be described hereinafter.

In step S1 a router receives one or more source path messages (SPMs) and adds the incoming interface IP address to it. If the router receives SPMs for more than router, it selects the SPM which was received first i.e. the one which provides the shortest route. In step S3

the router then determines the label from the SPM which comprises the received SPM and the added incoming interface IP address. In step S4 the outgoing interface IP address is then added to the SPM and this is transmitted over the interface. In step S5 the router then determines whether there are any more interfaces which requires the SPM message to be transmitted over. If so, the process returns to step S4.

Each router includes a random number generator as described later with reference to Figure 11. In step S6 a random number generator is initialised using the router label and the interface IP address as the key for each interface. The interface address is the IP address of the router on the interface to the next router or to a receiver. Where more than one router or receiver is connected to the router a unique random number sequence must be generated for segments passing down each connection and thus the psuedo random number generator must be initialised using a unique key for each connection. Thus a separate pseudo random number sequence is generated for each IP address (i.e. interface). The IP address provides the uniqueness indicating the path from the router and the router label provides the information identifying the router. Where the router is the last router in the route (the last "hop" router) and one or more receivers are connected to it, the random number generator key comprises not just the router label,

and the IP address on which the receiver is connected, but also the unique ID for the receiver e.g. the subscriber ID. In step S7 the router is then ready to receive the information signal and carry out the filtering (selection) procedure using the random number generator as the selector to determine which packets pass through the router.

The last hop router thus stores not just a label but also the receiver ID information for receivers connected to it. This information together with the source path message (SPM) is transmitted back to the source S to be stored for later analysis if necessary in order to determine the origin of illegal copies of the information signal.

The operation of a router when passing packets onto another router will now be described with reference to Figure 5a.

In step S10A packets arrive at the router. In step S11A the router waits until a whole transmission group i.e. all of the multiple copies for a segment are received. When the whole transmission group has been received, in step S12A one packet which is identified in the group by the random number generator is discarded. The remaining packets in the transmission group are then transmitted to the next router in step S13A. Thus a subsequent router will receive a transmission group which is smaller.

Figure 5b is a flow diagram illustrating the steps for forwarding data at a last hop router to a receiver. In step S10B packets arrive at the last hop router and the router waits in step S11B for the whole transmission group to be received. Once all packets of the transmission group have been received one of the packets which is identified by the value generated by the random number generator is selected in the group and in step S13B the selected packet is transmitted through the receiver. Thus, each receiver only receives one packet in a transmission group i.e. only one watermarked copy of each segment of the information signal.

An example of how an information signal is multicast over the network will now be described with reference to Figures 6, 7 and 8.

Figure 6 illustrates the data structure of the watermarked information signal generated at the source. A transmission group T comprises multiple differently watermarked versions of a segment of the information signal. In this embodiment there are five different watermarked versions A, B, C, D and E i.e. N=5. Each transmission group (1,2....P) is transmitted sequentially. As can be seen in Figure 6 the information signal is segmented into P segments and thus there are P transmission groups transmitted i.e. 5P packets.

As can be seen in Figure 8, the data structure of Figure 6 is received by the first node N_1. A random

number generator is initialised using the same label (1) for the node but using the interface IP addresses of each path to pseudo-randomly select one of the packets in each transmission group to be filtered out. Thus, nodes N_2 and N_3 receive transmission groups of length 4. Nodes N_4 and N_5 then receive transmission groups of length 3 and the furthest node N_6 receives a transmission group of length 2. At each of the nodes N_2, N_4, N_5 and N_6 which have receivers connected to them, a random number generator is initialised using the node label, the IP address and the receiver ID in order to select from each of the received transmission group one packet to be transmitted to the receiver. Thus each receiver receives only one packet for each segment. An example of the unique watermark sequence of segments is illustrated in Figure 7 for receiver R_1.

As can be seen from this example, each node in the network receives a transmission group of length N-D where D is the depth of the node along the route i.e. the number of previous nodes or "hops" through which the transmission groups have passed. The number of watermarked versions of each segment received at a node having a receiver must be at least 2 and thus the number of packets in a transmission group must therefore be at least D for the longest route to a receiver. If N >> D,

the number of segments required for the sequence of watermark segments to be unique is reduced.

Although not illustrated in Figures 6 and 7, each transmission group will contain headers indicating the number of segments in a transmission group. This is continuously changed at each node as the number of packets in a transmission group is reduced as the group passes through the network. Each packet within the transmission group also contains a header identifying its sequence in the transmission group. Once again this will need to be updated as packets are filtered out by routers e.g. if a router receives A, B, C, D, E and filters out D, E must be relabelled as the 4th packet in the transmission group.

Alternatively for packets which have been filtered out (deleted) a place holder packet can be transmitted indicating to subsequent routers that the packet has been intentionally discarded. This place-holder packet can be transmitted in conjunction with a following data packet to avoid the necessity to transmit a separate packet.

Multicast IP sessions allow subscribers to join and leave the sessions at any point i.e. midway through reception of an information signal. Also, the routes taken by the information signal through a network can change e.g. if a router fails. Thus, the source must continuously receive updated information on the paths taken by the information signal. This is achieved using

the source path message (SPM). The SPM is periodically broadcast over the network and information is received from the last hop routers connected to receivers giving route information to the source. If the route information indicates that the largest number of routers D in a path to a receiver is greater than or equal to the number of differently watermarked versions of each segment N, the source must increase the number of differently watermarked versions of each segment so that N > D. Also, if the longest route shortens and thus D is reduced, the bandwidth required for the transmission of the watermarked information signal over the network can be reduced by reducing N whilst still maintaining the relationship N > D. Thus the source monitors the network in order to monitor the routes to the receivers. If the number of differently watermarked versions of each segment is changed, the time at which it is changed i.e. the segment of the information signal at which the change takes place, is stored since this will affect the sequence of watermarked segments at each receiver.

The method by which a new subscriber to an IP multicast session can join the session will now be described with reference to Figure 9.

In step S20 the source assigns subscribers unique IDs and stores subscriber information. The receiver acquires the subscriber ID from the source. In step S21 the new subscriber contacts the nearest router (last hop

router) and communicates to it the unique subscriber ID which is required in order to join the multicast session. In step S22 the router then waits for receipt of the SPM, if it has not already received it. The router then sends to the source in step S23 the source path message (SPM) which indicates the route to the router, the subscriber ID identifying the new receiver, and the ID of the first data packet which is sent to the receiver i.e. an identification of the time at which the receiver first started to receive the copy of the information signal. This information is stored at the source for later use if necessary in order to identify the source of an illegal copy of the information signal.

At the source, in step S24 the new depth d of the network for the new subscriber is determined from the source path message (SPM). In step S25 it is determined whether this new depth is larger than the current depth i.e. is $d > D$. If so, in step S26 the source increases the number of differently watermarked versions of each segment N to maintain the relationship $N > d$ and in step S27 the last hop router then receives and forwards the information signal to the receiver. If in step S25 it is determined that the new depth is no greater than the current depth D used by the source to determine N, in step S27 the last hop router receives and forwards the information signal to the receiver. It should be noted here that the last hop router before the receiver will

not transmit packets to the receiver unless it receives multiple copies to choose from. This is necessary in order to avoid a number of receivers connected to the last hop router receiving the same sequence of watermarked segments. The last hop router must receive at least two differently watermarked copies of each segment so that the pseudo random number generator can be used to randomly select from these for a number of receivers which may be connected to the router so that each receiver receives a unique sequence of watermarked segments.

In this embodiment in addition to the use of differently watermarked versions of each segment, conventional IP multicast security techniques can be used such as encryption of the input information signal. A subscriber will be provided with the key to enable them to decrypt the information signal. The key for the encryption is usually common to all receivers of the multicast session. Within the packets, headers used for identifying the number of packets in a transmission group and for identifying the packet sequence in the transmission group are not encrypted since the routers need to use the header information for the filtering process.

In effect, the tree topology together with the receiver ID is the secret used by the source to perform the watermarking. Participating routers should therefore

refuse requests to reveal any part of that topology. Even if some routers and clients collude, it would need a conspiracy from a client right up to the source to discover anything useful.

The selective discard function aims to provide the multicast routers and their clients with the minimum degree of freedom possible in order to facilitate the later tracing of cheating routers or users. Every router in the tree indelibly affects the stream by dropping certain packets; thus a cheating router should be identifiable as every user downstream from that router would need to collude to reproduce the watermark data passing through the router.

The higher up the tree, the less likely it is; the lower down the tree the easier to eliminate targets from an investigation. Introducing redundant data into the multicast stream increases the size of the stream by the number of packets per transmission group at the first hop router, then one less at the second hop router and so on until the packets reach the receiver where the traffic size is the same as for a non-watermarked stream. Where N is the group size and H is the maximum number of "hops" in the tree from the source to the receiver (i.e. H=D+1), this increases the amount of traffic by a factor of:

$$\frac{2N-H+3}{2}-\frac{N}{H}$$

This is still far less than the traffic that would be generated by unicasting the unique version in each stream to every receiver. If N=H, which creates the minimum extra traffic but takes the watermark sequence longer, this factor is:

$$\frac{H+1}{2}$$

When the last hop router connects to a sub-network (local area network) such as an ethernet, any host on that network can receive the same packets with no extra effort. Non-subscribers on a network can intercept such packets, but do not have the decryption key needed to read them. However, two legitimate subscribers on the same sub-network will receive the same watermarked data. This however, is typically not a problem since multiaccess sub-networks are typically under the administrative control of a single agency. If one of the users of such a network illegally copies the information signal, it is traceable to the agency controlling that network and this is sufficient in most cases.

The source of this embodiment to the present invention can comprise any suitably programmed computer with network access. A schematic diagram of the structure of such an apparatus will now be described with reference to Figure 10.

All the components of the apparatus are linked by a computer bus 20. The computer apparatus includes a read-only memory (ROM) 22 which contains the conventional bios for the computer system. Random access memory (RAM) 21 is provided as the working memory to be used by a processor 23 during the processing operations. The processor 23 accesses a storage device 24 in order to load up programs to implement a watermarking application 23a, an encryption application 23b, a network monitoring application 23c and an analyser application 23d. The watermarking application 23a carries out the segmentation and watermarking of the segments to generate a plurality of differently watermarked copies of each segment using watermarking parameters stored in the storage device 24 together with information on the depth of the tree D i.e. to determine the number N of differently watermarked copies of each segment generated. The encryption application 23b carries out conventional encryption of the watermarked segments for transmission over the network. The network monitoring application 23c carries out monitoring functions in order to receive information from the network on routes to receivers, receiver IDs', information on the depth of the tree, which can be retrieved from the source path message (route information), and the times when receivers receive the first segments i.e. an identification of the first segments received by the receivers. This information is

then stored in the storage device 24. The processor 23 also implements a program module from the storage device 24 in order to implement an analyser application 23d for the analysis of a watermarked copy of an information signal in order to determine the receiver or receivers from which it originated. This process will be described in more detail hereinafter. A removable memory device 33 is provided to enable the copy of the information signal to be analysed to be input. Such a removable memory device 33 can for example be a floppy disk drive or CDROM. Alternatively, the copy of the information signal to be analysed can be input over the network 30 via the network interface 25.

The information signal to be multicast can be obtained from an information source in the form of a database 26, or it can be obtained real time via an input/output device 27 which is connected to, in this example, a video camera 28. Thus the information signal input from the input/output device 27 or the database 26 is watermarked by the watermarking application 23a operated by the processor 23 and encrypted by the encryption application 23b before being multicast over the network 30 by the network interface 25.

The computer apparatus is also provided with a conventional display 29, a keyboard 31 and a pointing device 32 to allow a user to interface with the computer apparatus.

Thus within the source, the storage device 24 stores:

1. The subscriber ID;
2. The time the subscriber joined (and left) the multicast session;
3. The route to the subscriber;
4. N for each segment; and
5. The watermarking scheme and parameters that are used for each packet.

Also a copy of the multicast information signal is either stored in the storage device 24 or a reference to its storage location in the database 26 is stored.

Other parameters which are stored in the storage device 24 are: a database of valid users so that when a request is made during a multicast session the validity of the request can be checked, and data on the encryption scheme used to encrypt the multicast information signal. Watermarked segments will be stored temporarily in the RAM 21. Instead of storing the watermarking scheme, and parameters used for each packet and a copy of the original information signal in the storage device 24, the watermarked segments can be stored. The storage device 24 also stores the multicast addresses to be used for the multicast session or sessions and the transmission protocol. Further, if the information signal is compressed or encoded, information on the compression or encoding scheme is stored.

A functional diagram of the functional components of a router 40 used in the network 30 for switching the information signal over routes in the network will now be described with reference to Figure 11. Many of the functions illustrated and described hereinafter are implemented by a processor operating in accordance with processor instructions.

The router 40 is provided with a first interface 41 which receives data from either another router further up the tree or from the source. Also SPMs' are received and transmitted. Received data is passed through a filter module 42 for filtering the data to remove at least one of the packets in a transmission group. The filter module 42 operates under the control of a random number generator (RNG) 43. The random number generator 43 is initialised using parameters stored in a volatile memory 44. The volatile memory 44 stores a label for the router, the IP address for each interface and the current state of the random number generator 43. Data is thus filtered by the filter module 42 and is output to the second interface 45 and the third interface 46. SPM's are received by the interface 41 and are utilised by the pragmatic general multicast (PGM) protocol engine 47. The PGM protocol engine 47 adds the IP address of the router 40 to the SPM and returns the SPM to the source via the interface 41. It also passes the SPM message to the second and third interfaces 45 and 46 for output to the

next routers or the receivers. The router 40 also includes a subscription manager 48 for managing subscriptions by receivers. If any router 40 is thus the last hop router in a route and has a receiver connected to it, when a receiver wishes to join an IP multicast session, subscriptions messages (SM's) are sent to the respective interface 45 or 46 and are then passed to the subscription manger 48. The subscription messages include the subscriber ID and this is stored in the volatile memory 44 for use in addition to the router label and the interface IP address for the initialisation of the random number generator 43 for an interface to the receiver. Also the subscriber ID in a volatile memory 44 is passed back to the source. The subscription messages also include requests to join and leave a multicast session.

In the embodiment of Figure 11, the PGM protocol can be replaced with any suitable protocol e.g. general multicast transport service (GMTS).

An analysis method for analysing a watermarked copy of the information signal in order to identify its origin i.e. to identify a router or receiver which received the sequence of watermark segments, will now be described with reference to the flow diagram in Figure 12. In this flow diagram the sequence of packets are analysed sequentially and at each point in the sequence it is

determined which recipients could have received the packet. A group of "culprits" is therefore determined. If there is a direct match between the sequence predicted for a subscriber or a router this is clearly the most likely culprit.

In step S30 a packet is selected and in step S31 all recipients of packets i.e. both routers and users are marked as suspects. This list of suspects will be reduced during the following steps in order to try to predict the most likely suspect.

In step S32 the operation starts by predicting the operation of the first hop router. In step S33 the next interface on the list of suspects at the router is considered and in step S34 it is determined whether the random number generator is initialised for this interface on this node. If not in step S35 the random number generator is initialised with the router label and the interface ID (and for the last router also the subscriber ID). In step S36 the random number generator is then run to determine the packet sequence. In step S37 it is then determined whether the router sent the packet on this interface. If so in step S38 it is determined whether there is a router at the end of the interface. If so, the process moves down the tree in step S39 to the router at the end of the interface and the process returns to step S33. If in step S38 it is determined that a

receiver is at the end of the interface the process then moves on to step S41.

If in step S37 it is determined that a router did not send the packet, in step S40 the interface and all its children are removed from the list of suspects. Then in step S41 it is determined whether there are any remaining suspected interfaces on the router. If so the process returns to step S33. If not in step S42 it is determined whether the router being considered is the first hop router. If not in step S43 the parent router is then considered and the process returns to step S41. In this way by continuously looping in steps S41, S42 and S43 the tree can be traversed back up to the first hop router.

If in step S42 it is determined that the router being considered is the first hop router, then the whole of the tree will have been traversed for the selected packet and thus in step S44 it is determined whether this is the last packet. If not, the process returns to step S30 to be repeated for the next packet. If all of the packets have been considered, in step S45 the union of the set of suspects is then found as the group of likely culprits.

This method will identify more than one culprit if the information signal has been patched together from the sections from different receivers trying to get round the watermarking security measure. Because the comparison

is done packet by packet, the receivers who colluded to generate the illegal copy will be identifed.

This technique enables the identification of not only the receivers but also any routers from which illegal copies could have originated.

OTHER EMBODIMENTS

Although the embodiment of the present invention has been described with reference to IP multicast over the Internet or an intranet, the present invention is applicable to any form of network such as a cable network which has some intelligence capability in the network switches.

In IP multicast, the protocol allows a maximum number of 32 nodes in a route and thus the depth D is limited. This limits the number of multiple different watermarked versions of a segment which needs to be generated and transmitted over the IP multicast system. The present invention is, however, applicable to any network and benefits from the present invention are obtained so long as the number of nodes in the network are less than the number of receivers.

Although the present invention is particularly suited to multicast transmissions over a network wherein the selection process is carried out within the network, the present invention provides advantages for unicast transmission since it reduces the processing required by

the information signal source. Fewer watermarked copies of the information signal need be generated and the unique sequence of watermarked segments for each user can be provided by a simple selection or filtering process.

Further advantages of the present invention can still be provided in non-networked systems where in effect D=1. The technique still benefits from a reduction in the number N of watermarked copies which have to be produced.

Although in the claims the system is stated as being implemented by discrete means, any of the means can be combined in an implementation of the system. For example, the present invention is ideally suited for implementation in software on a multi-purpose computer. Thus, the segmentation, watermarking and selection means can be embodied as instructions for controlling a processor. In the network embodiment the segmentation and watermarking means are implemented by software at a source's computer and the selection means is implemented by software in each of the routers in the network. Because the present invention can be implemented as software controlling a multi-purpose computer, the present invention can be embodied as a storage medium such as a CD-ROM, floppy disc, solid state memory device, or tape on which are stored instructions in the form of computer codes for controlling a processor to carry out the process. Further, the computer code can be

transmitted over a network to be installed on a computer to allow it to implement the invention, and thus the present invention is also embodied as a signal carrying the computer code.

The watermarking technique used to form the differently watermarked versions of each segment can comprise the same watermarking technique using different watermarking parameters, or different watermarking techniques. Different watermarking techniques can be used so long as they do not perceivably affect the data.

Although in the embodiment of Figures 5a and 5b the routers await reception of a whole transmission group before filtering, the filtering or selection process need not await the receipt of a whole transmission group.

Further, the selection process is not limited to the use of a pseudo random selection procedure, and anything which will give a plurality of deterministic sequences keyed by receiver information can be used.

Although specific embodiments of the present invention have been described hereinabove with reference to the drawings, the present invention is not limited to such embodiments and it will be apparent to a skilled person in the art that modifications can be made which lie within the spirit and scope of the invention.

CLAIMS

1. A method of watermarking an information signal to generate multiple different watermarked copies of the information signal, the method comprising:

segmenting the information signal into information segments;

generating a plurality of differently watermarked versions of each information segment; and

selecting one of said watermarked versions for each segment for each one of the multiple different copies to be generated to generate a sequence of differently watermarked segments which is different for each copy.

2. A method according to claim 1, wherein the selecting is performed using information on the receiver of each copy such that the sequence of differently watermarked segments of each copy is dependent upon the receiver of the copy.

3. A method according to claim 2, wherein the selecting is performed pseudo-randomly based on receiver identification information.

4. A method according to claim 2 or claim 3, wherein the information on the receiver includes at least one of

unique identification information for the receiver and information on the location of the receivers.

5. A method according to any preceding claim wherein the copies of the information signal are transmitted to recipients over a network, and the selecting is performed in dependence upon the route taken for each copy to reach a respective recipient.

6. A method according to claim 5, wherein said network comprises a plurality of switching means for switching the route taken by information in said network, the generated plurality of differently watermarked versions of each information segment are generated at an information source and input to said network, and said switching means carry out the selecting by selecting from received watermarked versions for each segments at least one watermarked version for each segment not to be transmitted on.

7. A method according to claim 6, wherein said switching means to which other said switching means are connected in the network select one of the received watermarked versions for each segment which is not to be transmitted onto the other said switching means.

8. A method according to claim 6 or claim 7, wherein said switching means to which one or more recipients are connected selects one of the received watermarked versions for each segment which is the watermarked version for the segment to be transmitted to each recipient connected to the switching means.

9. A method according to any one of claims 6 to 8, wherein the number of differently watermarked versions of each segment generated is dependent upon the largest number of said switching means in a route between the source and a said recipient.

10. A method according to claim 9, wherein the number of differently watermarked versions of each segment is greater than the largest number of said switching means in a route between the source and a said recipient.

11. A method according to claim 9 or claim 10, wherein the number of said switching means in the routes from the source to the recipients are monitored and the number of differently watermarked versions of each segment varied in dependent upon the monitored number of said switching means.

12. A method according to any one of claims 6 to 11, wherein each said switching means which transmits to

another said switching means makes the selection based on the position of the switching means in the route from the source to the recipients.

13. A method according to any one of claims 6 to 12, wherein each said switching means which transmits to a recipient makes the selection based on unique identification information for the recipient.

14. A method according to any one of claims 6 to 13, wherein each said switching means transmits information on the position of the switching means in the route between the source and the recipients to said source.

15. A method according to claim 13, wherein each switching means which transmits to a recipient receives information on the identity of the recipient from the recipient and transmits this to said source.

16. A method according to any preceding claim wherein each watermarked version of each segment is watermarked using the same watermarking technique and is watermarked differently.

17. A method according to any one of claims 1 to 15, wherein each watermarked version of each segment is

watermarked using one of a number of possible watermarking techniques.

18. A system for watermarking an information signal to generate multiple different watermarked copies of the information signal, the system comprising:

segmenting means for segmenting the information signal into information segments;

watermarking means for generating a plurality of differently watermarked versions of each information segment; and

selecting means for selecting one of said watermarked versions of each segment for each one of the multiple different copies to be generated to generate a sequence of differently watermarked segments which is different for each copy of the information.

19. A system according to claim 18, wherein said selecting means is adapted to perform the selecting using information on the receiver of each copy of the information signal to produce the sequence of differently watermarked segments of each copy dependent upon the receiver of the copy.

20. A system according to claim 19, wherein said selecting means is adapted to perform the selection

pseudo-randomly based on receiver identification information.

21. A system according to claim 19 or claim 20, wherein said selecting means is adapted to perform the selection using at least one of unique identification information for the receivers and information on the location of the receivers.

22. A system according to any one of claims 18 to 21, wherein said selecting means comprises nodes in a network arranged to receive differently watermarked versions of each information segment and to generate the sequence of differently watermarked segments which is different for each copy in dependence upon the route taken for each copy to reach a respective recipient.

23. A system according to claim 22, wherein each node in the network is arranged to control the routing of the information signal within the network, said segmenting means and said watermarking means are provided at an information source connected to a first node in said network, said first node is adapted to receive the plurality of differently watermarked versions of each segment, said nodes are adapted to select from received watermarked versions for each segment at least one

watermarked version for each segment not to be transmitted on.

24. A system according to claim 23, wherein said nodes to which other said nodes are connected are adapted to select one of the received watermarked versions for each segment which is not to be transmitted on to the other nodes.

25. A system according to claim 23 or claim 24, wherein said nodes to which one or more recipients are connected are adapted to select one of the received watermarked versions for each segment which is to be transmitted on to each recipient connected to the nodes.

26. A system according to any one of claims 23 to 25, wherein said watermarking means is adapted to generate the number of differently watermarked versions of each segment dependent upon the largest number of nodes in the routes between the source and the recipients.

27. A system according to claim 26, wherein said watermarking means is adapted to generate the number of differently watermarked versions of each segment being greater than the largest number of said nodes in any of the routes between the source and the recipients.

28. A system according to claim 26 or claim 27, including monitoring means for monitoring the number of said nodes in the routes between the source and the recipients, wherein said watermarking means is responsive to said monitoring means to vary the number of differently watermarked versions for each segment generated in dependence upon the monitored number of said nodes.

29. A system according to any one of claims 23 to 28, wherein said nodes which transmit to another said node are adapted to make the selection based on the position of the node in the routes from the source to the recipients.

30. A system according to any one of claims 23 to 29, wherein said nodes which transmit to a recipient are adapted to make the selection based on unique identification information for the recipients.

31. A system according to any one of claims 23 to 30, wherein each said node is adapted to transmit information on the position of the node in the routes between the source and the recipients to said source.

32. A system according to claim 30, wherein each said node which transmits to a recipient is adapted to receive

information on the identity of the recipient from the recipient and to transmit the information to said source.

33. A system according to any one of claims 18 to 32, wherein said watermarking means is adapted to watermark each version of each segment using the same watermarking technique.

34. A system according to any one of claims 18 to 32, wherein said watermarking means is adapted to watermark each version of each segment using one of a number of possible watermarking techniques.

35. Apparatus for watermarking an information signal comprising:

segmenting means for segmenting the information signal into information segments; and

watermarking means for generating a plurality of differently watermarked versions of each information segment.

36. Apparatus according to claim 35, including interface means for connection to a node in a network, wherein receivers requiring a copy of the information signal are connected to nodes in the network and the nodes in the network select one of the watermarked versions for each segment for each receiver to generate a sequence of

differently watermarked segments which is different for each receiver, the apparatus including storage means for storing information on the receivers and information on the routes taken to transmit copies of respective receivers, wherein such interface is adapted to receiver said information over the network.

37. Apparatus according to claim 35, wherein said watermarking means is adapted to store parameters used to watermark each version of each segment.

38. Apparatus according to claim 36 or claim 37, wherein said interface means is adapted to receive from the network information indicating when a said receiver began to receive a copy of the information signal and to store the information in said storage means.

39. Apparatus according to any one of claims 36 to 38 wherein said interface is adapted to receive information identifying the number of nodes in the network between the apparatus and each receiver, and said watermarking means is adapted to set the number of differently watermarked versions of each segment in dependence upon the largest number of nodes identified between the apparatus and a receiver.

40. Apparatus according to claim 39, wherein said storage means is adapted to store the number of versions of watermarking used for each segment.

41. Apparatus according to any preceding claim wherein said storage means is adapted to store information identifying a storage location of the information signal or to store the information signal.

42. An apparatus according to all of claims 35 to 41, including analysis means for receiving a copy of an information signal having a sequence of differently watermarked segments to be tested and for using the information in said storage means to calculate the sequence of differently watermarked segments for said receivers for comparison with the sequence of differently watermarked segments to be tested to determine if there is a match between at least a portion of the sequences.

43. A method of watermarking an information signal at a source, the method comprising:

segmenting the information signal into segments; and

generating a plurality of differently watermarked versions of each information segment.

44. A method according to claim 43, including storing information on receivers of copies of the information

signal and information on the routes taken to transmit copies to respective receivers over a network having nodes which select one of the watermarked versions for each segment for each receiver connected to a node to generate sequence of differently watermarked segments which is different for each receiver.

45. A method according to claim 44, including storing parameters used to watermark each version of each segment.

46. A method according to claim 44 or claim 45, including receiving from the network information indicating when a said receiver began to receive a copy of the information signal and storing the information.

47. A method according to any one of claims 44 to 46, including receiving from the network information identifying the number of nodes in the network between the source and each receiver, and setting the number of differently watermarked versions of each segment in dependence upon the largest number of nodes identified between the source and a receiver.

48. A method according to claim 47, including storing the number of versions of watermarking used for each segment.

49. A method according to any one of claims 48 to 38, including storing information identifying a storage location of the information signal or storing the information signal.

50. A method according to all of claims 43 to 49, including receiving a copy of an information signal having a sequence of differently watermarked segments to be tested, and using the stored information to calculate the sequence of differently watermarked segments for said receivers for comparison with the sequence of differently watermarked segments to be tested to determine if there is a match between at least a portion of the sequences.

51. Apparatus for use in the method of any one of claims 6 to 15, the apparatus comprising:

receiving means for receiving a plurality of differently watermarked versions of each of a plurality of information segments forming an information signal;

selecting means for selecting at least one watermarked version for each segment not to be transmitted on; and

transmitting means for transmitting the or each remaining watermarked version for each segment over the network.

52. Apparatus according to claim 50, wherein said selecting means is adapted to use information on the position of the switch apparatus in the network to control the selection.

53. Apparatus according to claim 52, wherein said selecting means is adapted to use information on the route used for transmission to control the selection.

54. Apparatus according to any one of claims 51 to 53, wherein said selecting means is adapted to use information identifying a receiver to control the selection to select only one watermarked version for each segment to be transmitted on, wherein the receiver is the final receiver of the information signal, and said transmitting means is adapted to transmit the selected watermarked version for each segment to the receiver.

55. Apparatus according to any one of claims 52 to 54, wherein said selecting means includes a pseudo-random number generator and is adapted to carry out the selection pseudo-randomly, wherein the information is used as a key to initiate the pseudo-random number generator.

56. Apparatus according to any one of claims 51 to 55, wherein said receiving means is adapted to receive a

message indicating the route the information signal will take, and said transmitting means is adapted to retransmit the message adding the identity of the apparatus in the route.

57. A method carried out at a node in a network, the method comprising:

receiving a plurality of differently watermarked versions of each of a plurality of information segments forming an information signal;

selecting at least one watermarked version for each segment not to be transmitted on; and

transmitting the or each remaining watermarked version for each segment over the network.

58. A method according to claim 57, wherein the selecting uses information on the route used for transmission to control the selection.

59. A method according to any one of claims 57 to 59, wherein the selecting uses information identifying a receiver to control the selection to select only one watermarked version for each segment to be transmitted on, where the receiver is the final receiver of the information signal, and the selected watermarked version for each segment is transmitted to the receiver.

61. A method according to any one of claims 58 to 60, wherein a pseudo-random number generator is used for the selection and is controlled using the information as a key to initiate the pseudo-random number generator.

62. A method according to any one of claims 7 to 61, including receiving a message indicating the route the information signal will take, and retransmitting the message adding the identity of the node in the route.

63. Apparatus for identifying the receiver of a copy of an information signal watermarked using the system of any one of claims 19 to 34, the apparatus comprising:

receiving means for receiving the copy of the watermarked information signal comprising a sequence of differently watermarked segments;

storage means for storing information on receivers of copies of the information signal;

accessing means for accessing the information signal;

determining means for determining watermarked versions for segments for receivers using the accessed information signal and the information on the receivers; and

matching means for matching the watermarks for segments for receivers with segments of the received copy of the watermarked information signal to identify the

receiver of the copy of the watermarked information signal.

64. Apparatus according to claim 63, wherein said storage means is adapted to store information on the nodes in a network forming the route between a source of the information signal and a receiver, and said determining means is adapted to determine the identity of the receivers using the route information.

65. A method of identifying the receiver of a copy of an information signal watermarked using the method of any one of claims 2 to 17, the method comprising:

receiving the copy of the watermarked information signal comprising a sequence of differently watermarked segments;

reading stored information on receivers of copies of the information signal;

accessing the information signal;

determining watermarked versions for segments for receivers using the accessed information signal and the read information on the receivers; and

matching the watermarks for segments for receivers with segments of the received copy of the watermarked information signal to identify the receiver of the copy of the watermarked information signal.

66. A method according to claim 64, including reading information on the nodes in a network forming the route between a source of the information signal and a receiver, and determining the identity of the receivers using the route information.

67. An information signal watermarked using the method of any one of claims 1 to 17 comprising a plurality of information transmission groups, each information transmission group comprising a plurality of differently watermarked versions of the same information packet.

68. A medium carrying the information signal of claim 67.

69. A signal carrying processor implementable instructions for controlling a processor to carry out the method of any one of claims 1 to 17, 43 to 50 or 57 to 62.

70. A storage medium carrying processor implementable instructions for controlling a processor to carry out the method of any one of claims 1 to 17, 43 to 50 or 57 to 62.

ABSTRACT

A METHOD AND APPARATUS FOR GENERATING MULTIPLE WATERMARKED COPIES OF AN INFORMATION SIGNAL

A method and apparatus for watermarking an information signal to generate multiple different watermarked copies of the information signal is disclosed. The information signal is segmented into information segments. The plurality of differently watermarked versions of each information segment is then generated and one of the watermarked versions for each segment is selected for each one of the multiple different copies to be generated to generate a sequence of differently watermarked segments which is different for each copy.

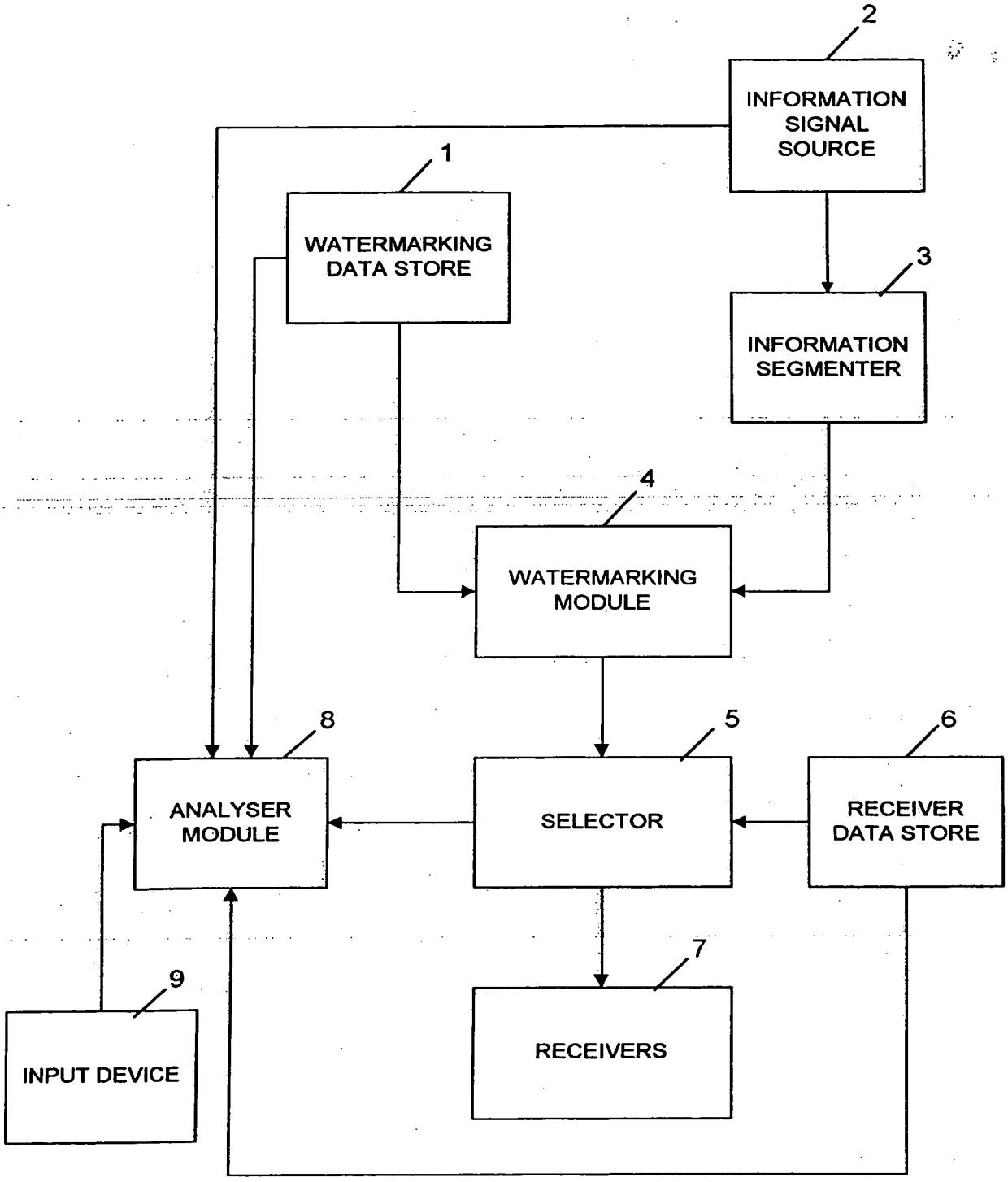

2
INFORMATION SIGNAL SOURCE
1
WATERMARKING DATA STORE
3
INFORMATION SEGMENTER
4
WATERMARKING MODULE
8
5
6
ANALYSER MODULE
SELECTOR
RECEIVER DATA STORE
7
9
INPUT DEVICE
RECEIVERS

Fig 1

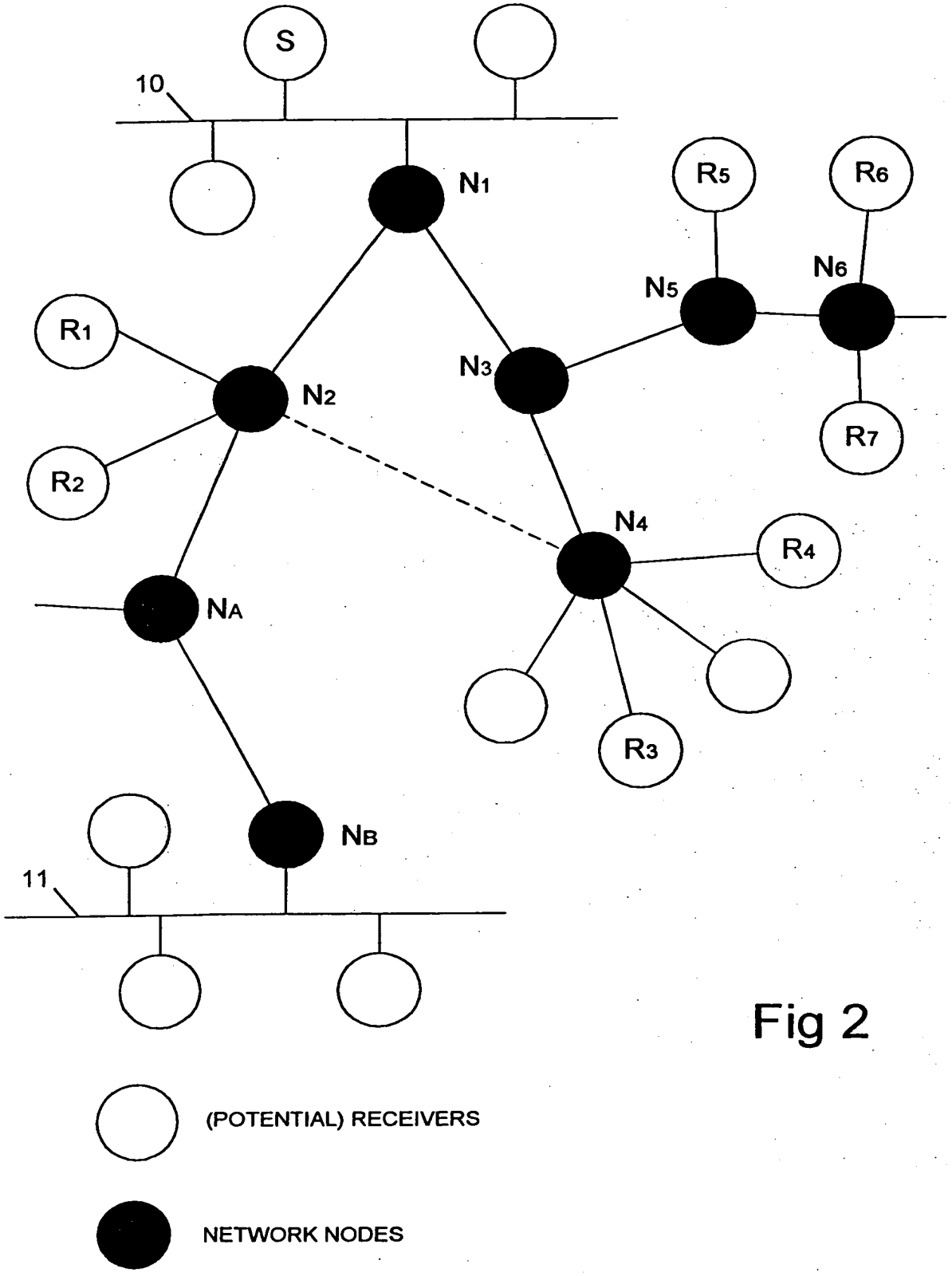

S
10
N1
R5
R6
N5
N6
R1
N3
N2
R7
R2
N4
R4
NA
R3
NB
11
(POTENTIAL) RECEIVERS
NETWORK NODES

Fig 2

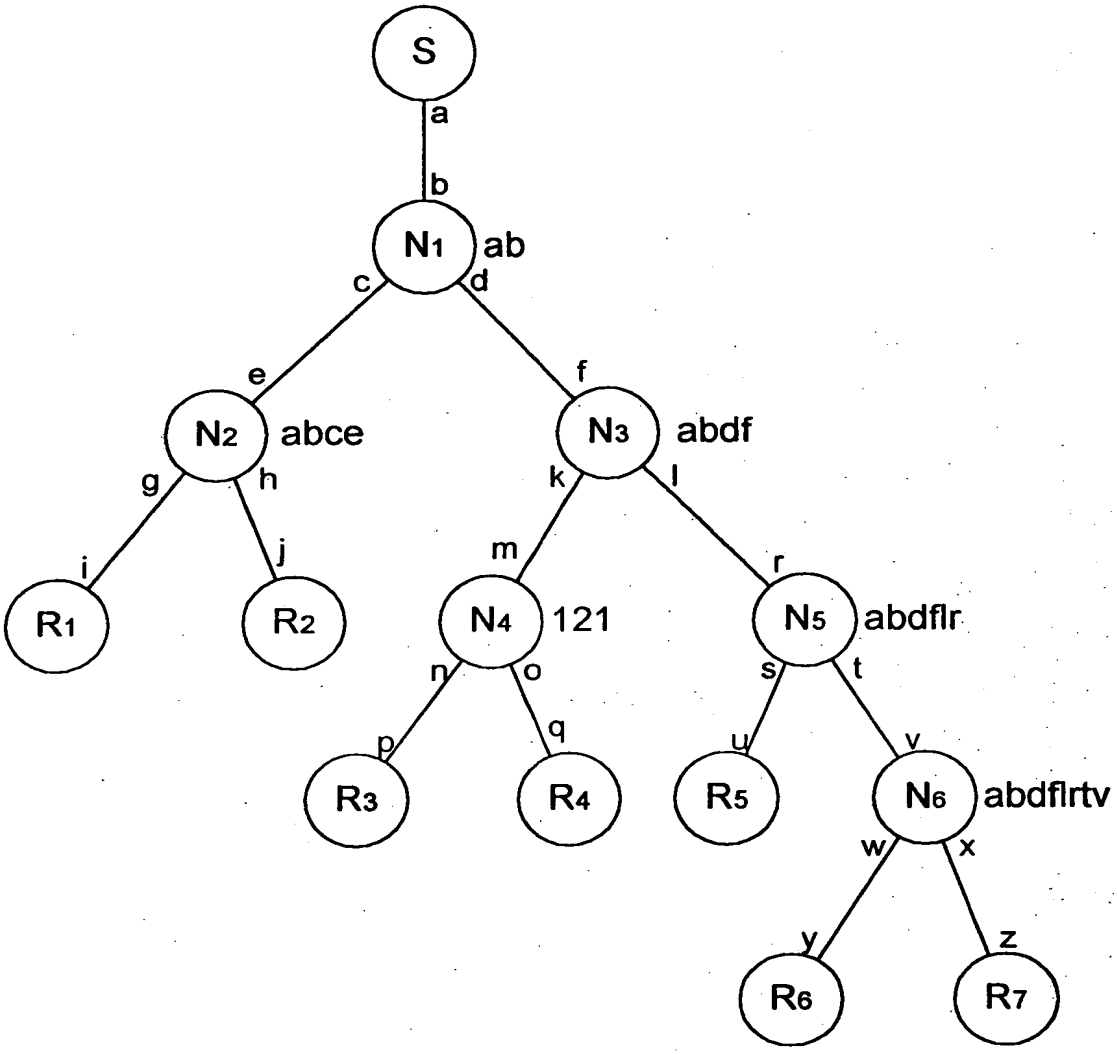

S
a
b
N1
ab
c
d
e
f
N2
abce
N3
abdf
g
h
k
l
i
j
m
r
R1
R2
N4
121
N5
abdflr
n
o
s
t
p
q
u
v
R3
R4
R5
N6
abdflrtv
w
x
y
z
R6
R7

Fig 3

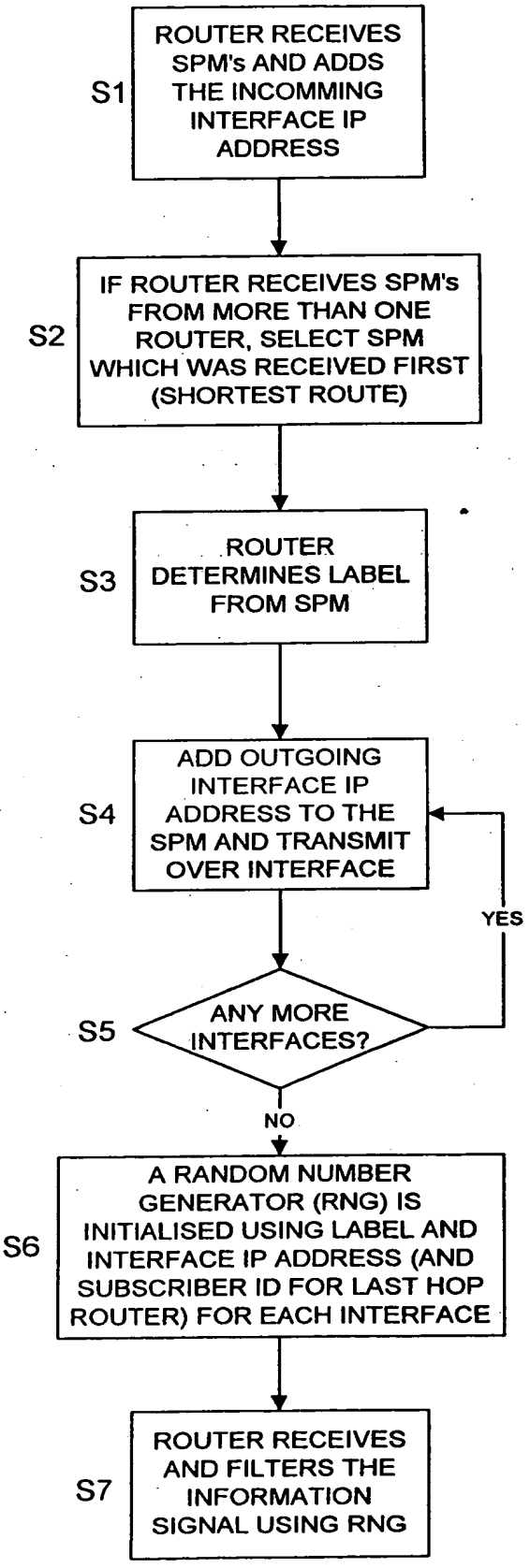

S1
ROUTER RECEIVES SPM's AND ADDS THE INCOMMING INTERFACE IP ADDRESS
S2
IF ROUTER RECEIVES SPM's FROM MORE THAN ONE ROUTER, SELECT SPM WHICH WAS RECEIVED FIRST (SHORTEST ROUTE)
S3
ROUTER DETERMINES LABEL FROM SPM
S4
ADD OUTGOING INTERFACE IP ADDRESS TO THE SPM AND TRANSMIT OVER INTERFACE
S5
ANY MORE INTERFACES?
YES
NO
S6
A RANDOM NUMBER GENERATOR (RNG) IS INITIALISED USING LABEL AND INTERFACE IP ADDRESS (AND SUBSCRIBER ID FOR LAST HOP ROUTER) FOR EACH INTERFACE
S7
ROUTER RECEIVES AND FILTERS THE INFORMATION SIGNAL USING RNG

Fig 4

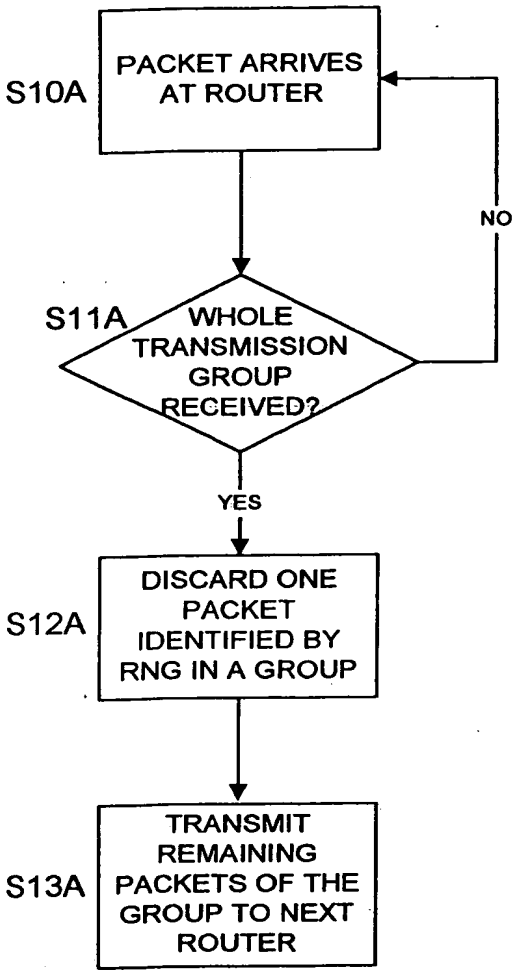

S10A
PACKET ARRIVES AT ROUTER
S11A
WHOLE TRANSMISSION GROUP RECEIVED?
NO
YES
S12A
DISCARD ONE PACKET IDENTIFIED BY RNG IN A GROUP
S13A
TRANSMIT REMAINING PACKETS OF THE GROUP TO NEXT ROUTER

Fig 5a

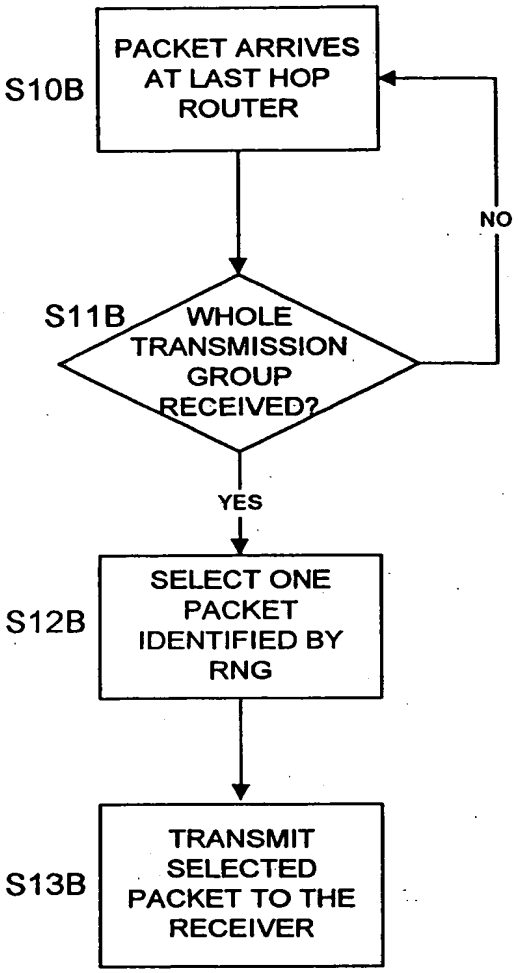

S10B
PACKET ARRIVES AT LAST HOP ROUTER
S11B
WHOLE TRANSMISSION GROUP RECEIVED?
NO
YES
S12B
SELECT ONE PACKET IDENTIFIED BY RNG
S13B
TRANSMIT SELECTED PACKET TO THE RECEIVER

Fig 5b

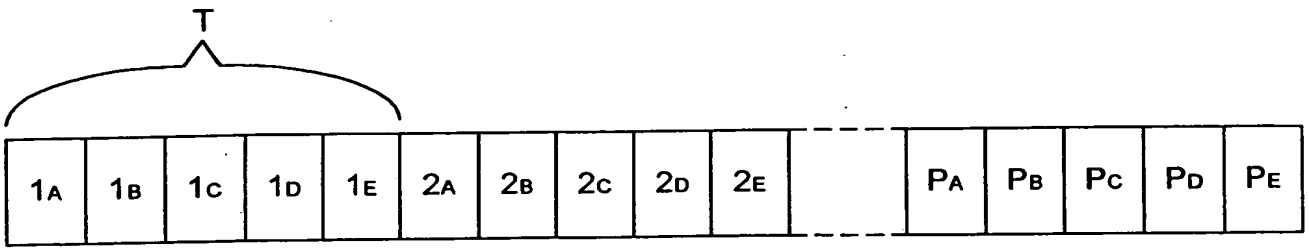

T
1A
1B
1C
1D
1E
2A
2B
2C
2D
2E
PA
PB
PC
PD
PE

Fig 6

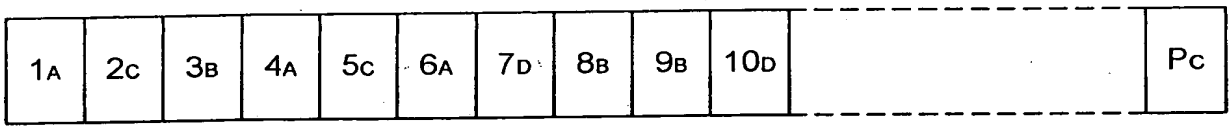

1A
2C
3B
4A
5C
6A
7D
8B
9B
10D
PC

Fig 7

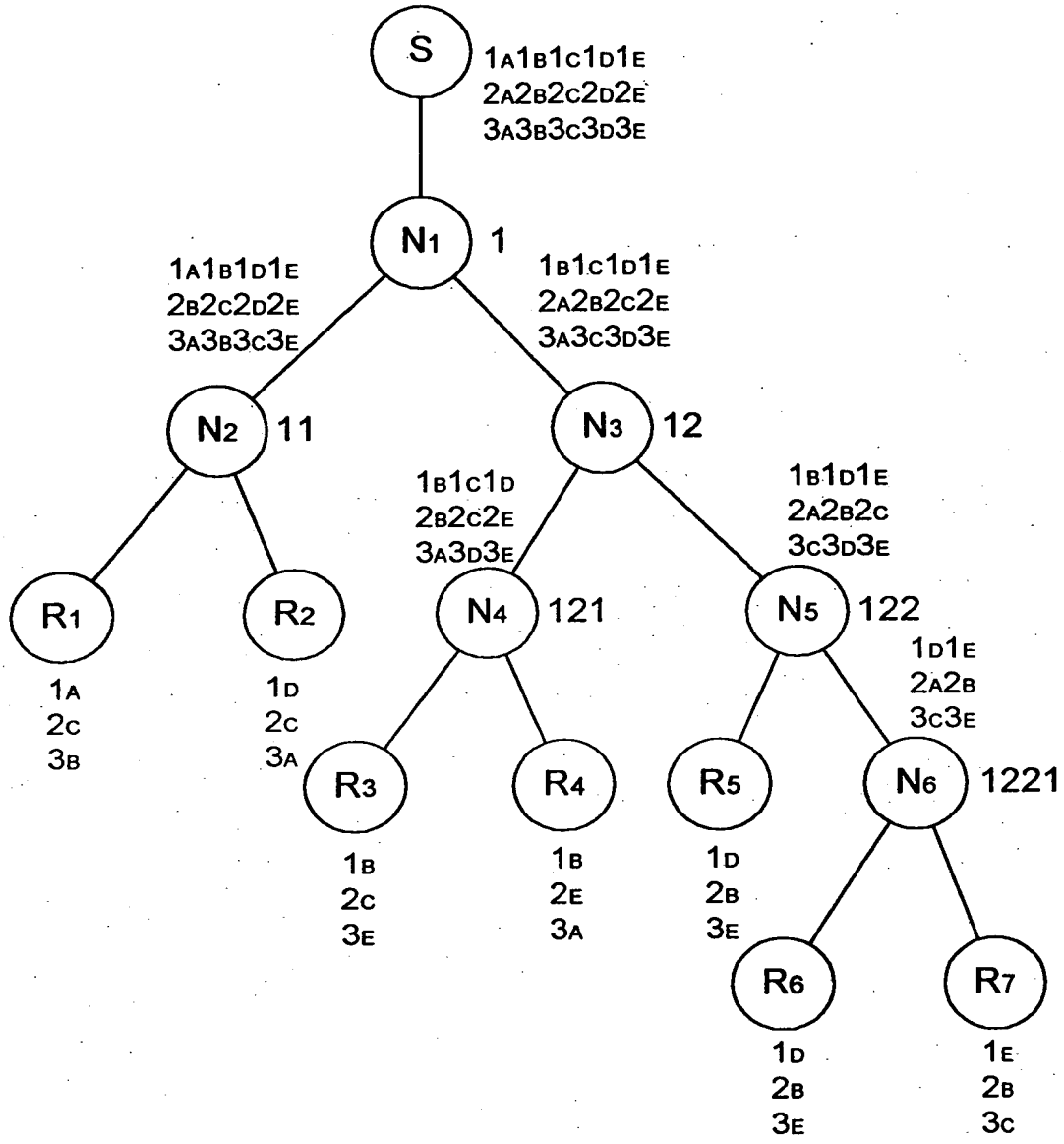

S
1A1B1C1D1E
2A2B2C2D2E
3A3B3C3D3E
N1
1
1A1B1D1E
2B2C2D2E
3A3B3C3E
1B1C1D1E
2A2B2C2E
3A3C3D3E
N2
11
N3
12
1B1C1D
2B2C2E
3A3D3E
1B1D1E
2A2B2C
3C3D3E
R1
1A
2C
3B
R2
1D
2C
3A
N4
121
N5
122
1D1E
2A2B
3C3E
R3
1B
2C
3E
R4
1B
2E
3A
R5
1D
2B
3E
N6
1221
R6
1D
2B
3E
R7
1E
2B
3C

Fig 8

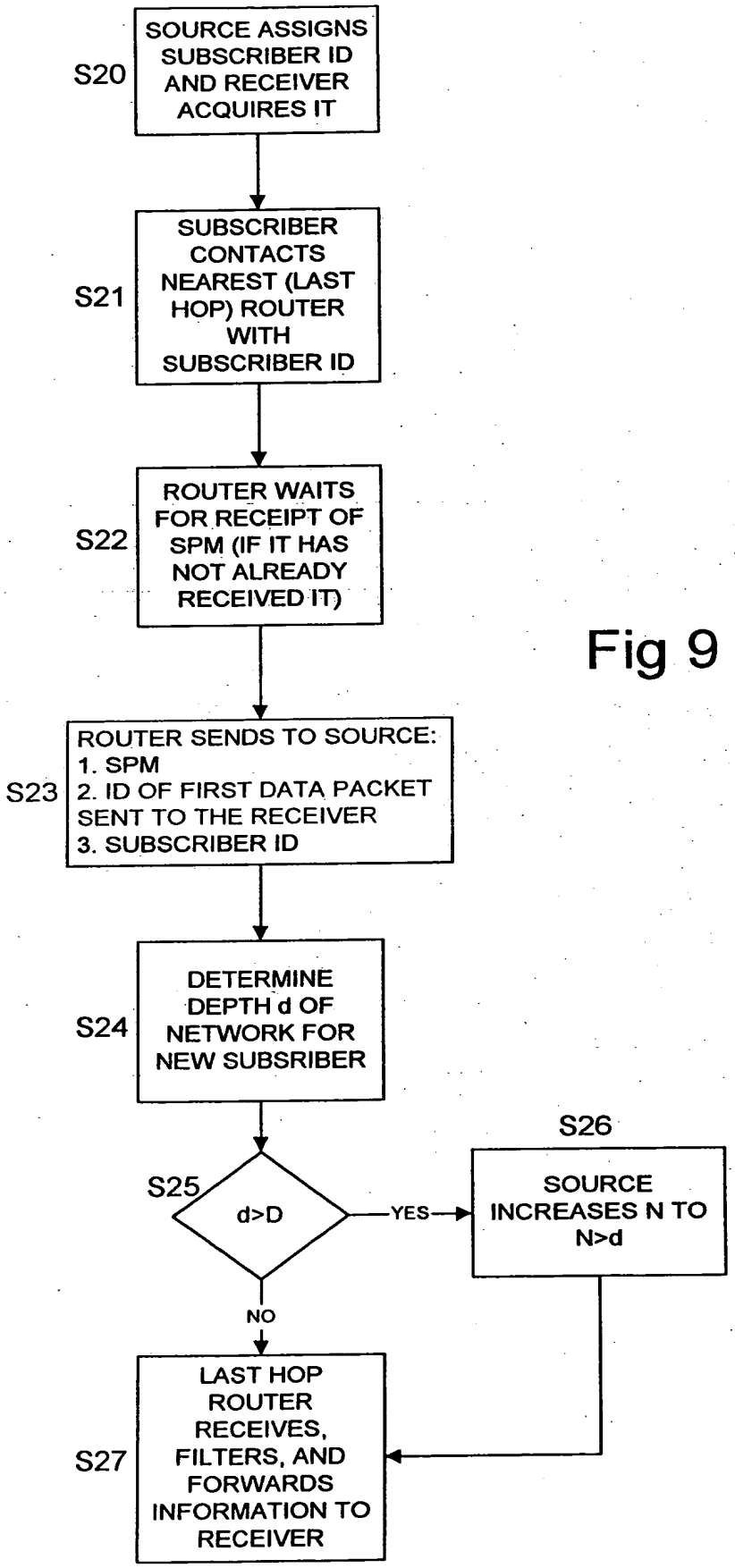

S20
SOURCE ASSIGNS SUBSCRIBER ID AND RECEIVER ACQUIRES IT
S21
SUBSCRIBER CONTACTS NEAREST (LAST HOP) ROUTER WITH SUBSCRIBER ID
S22
ROUTER WAITS FOR RECEIPT OF SPM (IF IT HAS NOT ALREADY RECEIVED IT)
S23
ROUTER SENDS TO SOURCE:
1. SPM
2. ID OF FIRST DATA PACKET SENT TO THE RECEIVER
3. SUBSCRIBER ID
S24
DETERMINE DEPTH d OF NETWORK FOR NEW SUBSRIBER
S25
d>D
YES
S26
SOURCE INCREASES N TO N>d
NO
S27
LAST HOP ROUTER RECEIVES, FILTERS, AND FORWARDS INFORMATION TO RECEIVER

Fig 9

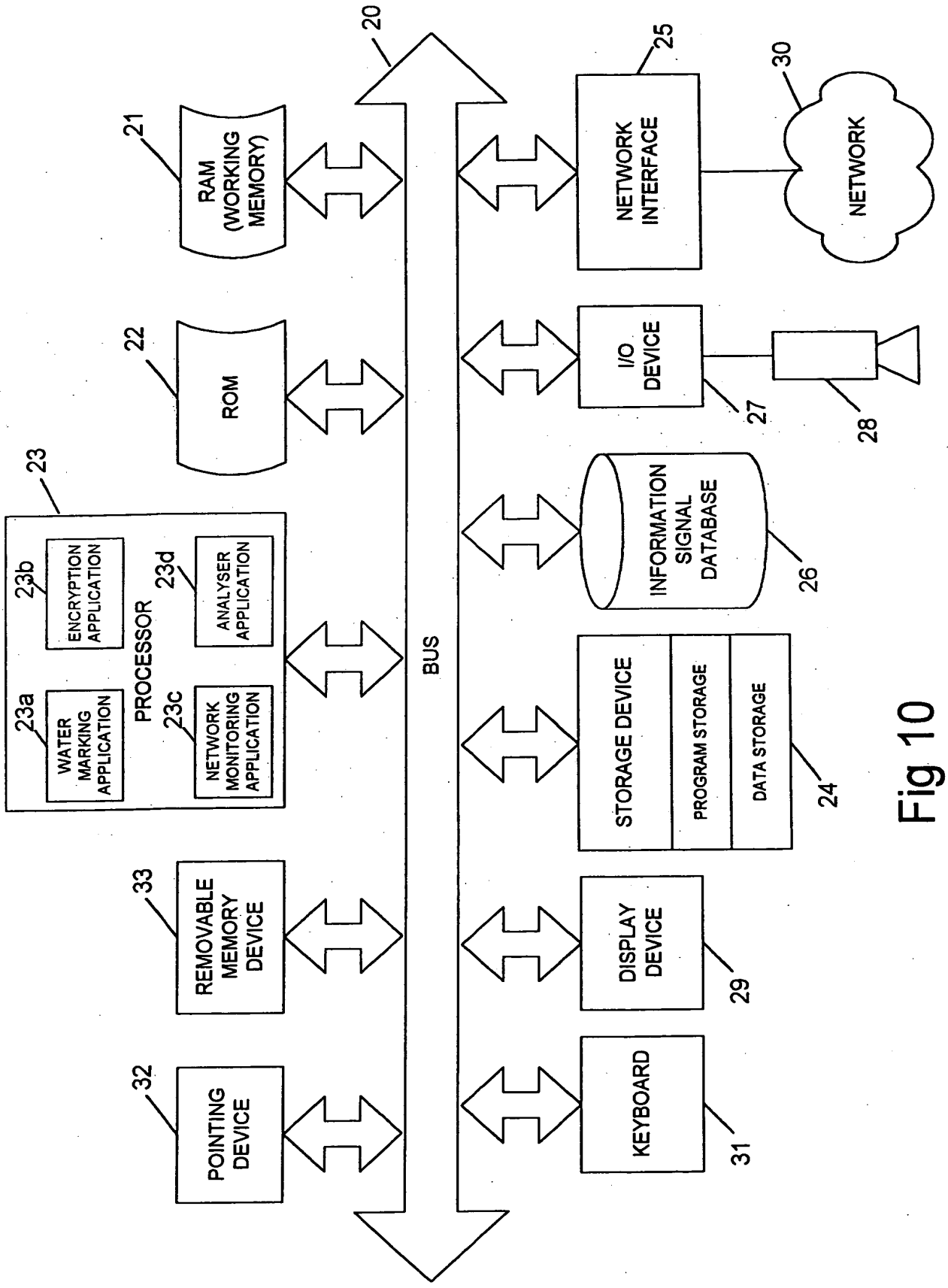

20
21
RAM (WORKING MEMORY)
22
ROM
23
PROCESSOR
23a
WATER MARKING APPLICATION
23b
ENCRYPTION APPLICATION
23c
NETWORK MONITORING APPLICATION
23d
ANALYSER APPLICATION
BUS
25
NETWORK INTERFACE
30
NETWORK
I/O DEVICE
27
28
INFORMATION SIGNAL DATABASE
26
STORAGE DEVICE
PROGRAM STORAGE
DATA STORAGE
24
33
REMOVABLE MEMORY DEVICE
DISPLAY DEVICE
29
32
POINTING DEVICE
KEYBOARD
31

Fig 10

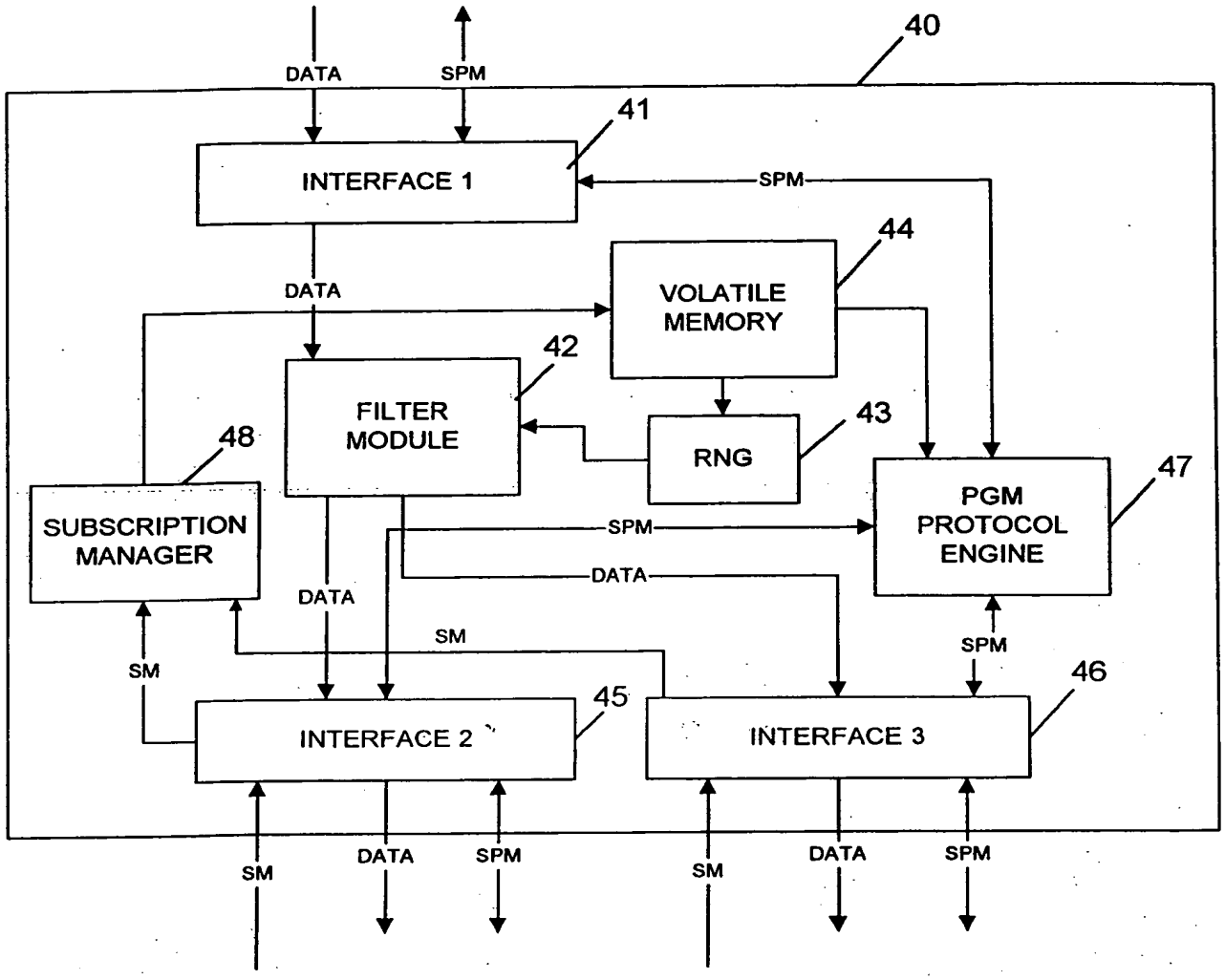

40
DATA
SPM
41
INTERFACE 1
SPM
44
DATA
VOLATILE MEMORY
42
FILTER MODULE
43
RNG
48
SUBSCRIPTION MANAGER
47
PGM PROTOCOL ENGINE
SPM
DATA
DATA
SM
SM
SPM
46
45
INTERFACE 2
INTERFACE 3
SM
DATA
SPM
SM
DATA
SPM

Fig 11

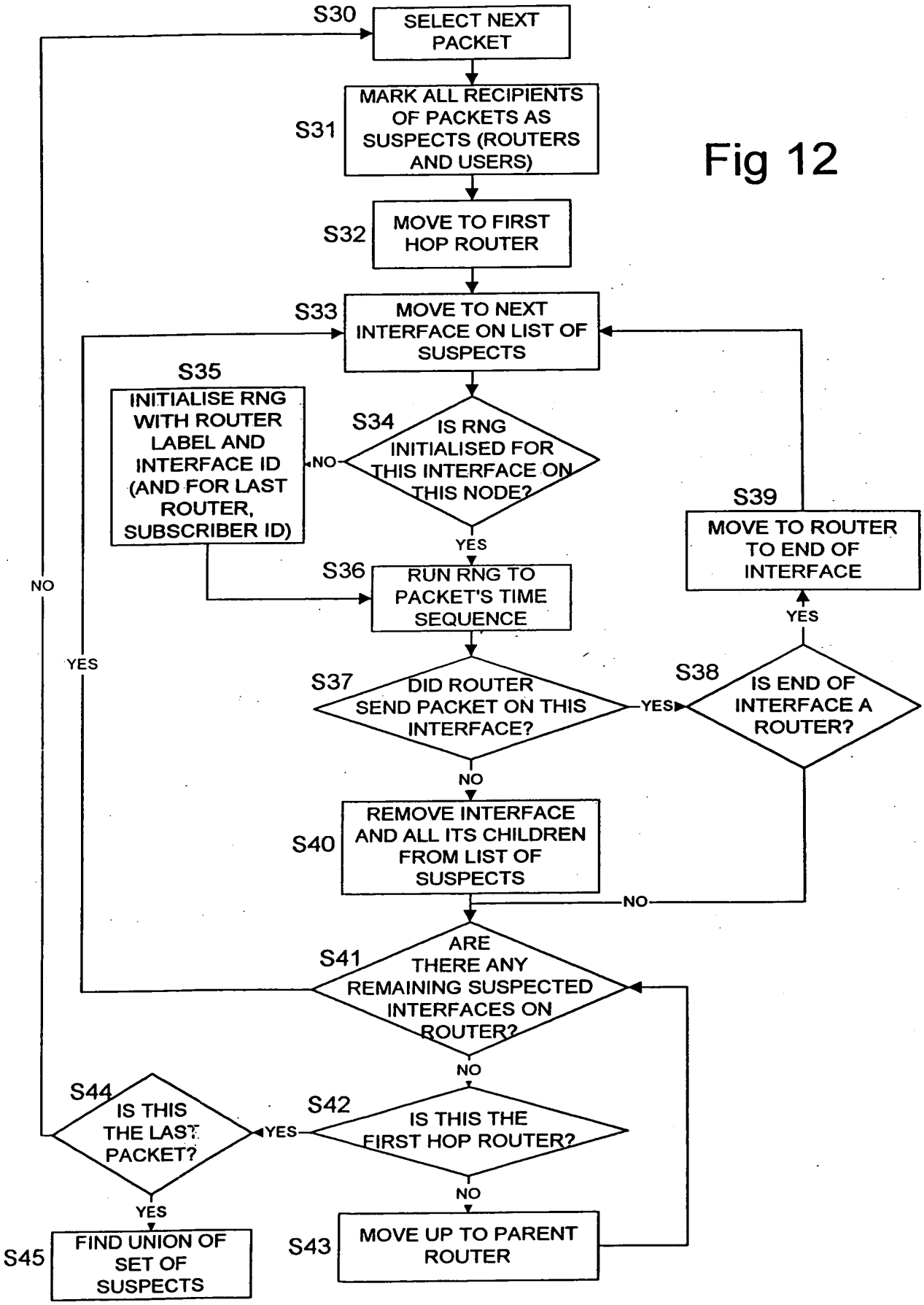

S30
SELECT NEXT PACKET
S31
MARK ALL RECIPIENTS OF PACKETS AS SUSPECTS (ROUTERS AND USERS)
S32
MOVE TO FIRST HOP ROUTER
S33
MOVE TO NEXT INTERFACE ON LIST OF SUSPECTS
S34
IS RNG INITIALISED FOR THIS INTERFACE ON THIS NODE?
NO
YES
S35
INITIALISE RNG WITH ROUTER LABEL AND INTERFACE ID (AND FOR LAST ROUTER, SUBSCRIBER ID)
S36
RUN RNG TO PACKET'S TIME SEQUENCE
S37
DID ROUTER SEND PACKET ON THIS INTERFACE?
YES
NO
S38
IS END OF INTERFACE A ROUTER?
YES
S39
MOVE TO ROUTER TO END OF INTERFACE
NO
S40
REMOVE INTERFACE AND ALL ITS CHILDREN FROM LIST OF SUSPECTS
NO
S41
ARE THERE ANY REMAINING SUSPECTED INTERFACES ON ROUTER?
YES
NO
S42
IS THIS THE FIRST HOP ROUTER?
YES
NO
S43
MOVE UP TO PARENT ROUTER
S44
IS THIS THE LAST PACKET?
YES
NO
S45
FIND UNION OF SET OF SUSPECTS

Fig 12

PCT/GB 00/00767

Bereford + Co,
London
23/3/00